STIC Search Report
EIC 2100

Scientific & Technical Information Center
USPTO

STIC Database Tracking Number: 119685

TO: Tran Tongoc **Location:** **Art Unit : 2134** **Monday, April 19, 2004** **Case Serial Number: 09/651424**	**From: David Holloway** **Location: EIC 2100** **PK2-4B30** **Phone: 308-7794** **david.holloway@uspto.gov**

Search Notes

Dear Examiner Tongoc,

Attached please find your search results for above-referenced case.
Please contact me if you have any questions or would like a re-focused search.

David

sira
Search and Information Resources Administration

11/4680

STIC EIC 2100
Search Request Form

Today's Date: 4-19-04

What date would you like to use to limit the search?

Priority Date: 8/30/2000 Other:

Name T. Tran

AU 2134 Examiner # 7999

Room # Pk2 4Y03 Phone 305-7690

Serial # 09/651424

Format for Search Results (Circle One):

PAPER DISK EMAIL

Where have you searched so far?

USP DWPI EPO JPO ACM IBM TDB

IEEE INSPEC SPI Other _____

Is this a "Fast & Focused" Search Request? (Circle One) YES NO

A "Fast & Focused" Search is completed in 2-3 hours (maximum). The search must be on a very specific topic and meet certain criteria. The criteria are posted in EIC2100 and on the EIC2100 NPL Web Page at http://ptoweb/patents/stic/stic-tc2100.htm.

What is the topic, novelty, motivation, utility, or other specific details defining the desired focus of this search? Please include the concepts, synonyms, keywords, acronyms, definitions, strategies, and anything else that helps to describe the topic. Please attach a copy of the abstract, background, brief summary, pertinent claims and any citations of relevant art you have found.

2 portion - Digital good

Select on

one portion encrypted

Unencrypted portion used as

key in substitute Box

S-Box

DES encryption

STIC Searcher Holloway Phone 305-7794

Date picked up 4-19-04 Date Completed 4-19-04

$623 1/2

DIALOG

50

```
Set     Items   Description
S1        633   SBOX? OR (SUBSTITUTION? OR S)()(BOX OR BOXES)
S2     149697   (BREAK? OR DIVID?)(2N)(TEXT OR DATA OR PLAINTEXT? OR IMAGE?
               OR DIGITAL()(GOOD? OR DOCUMENT? OR OBJECT? OR MEDIA?) OR MUL-
               TIMEDIA OR VIDEO OR STREAM) OR SPLIT? OR SUBDIVID?
S3     113652   (PORTION? OR PART? OR SECTOR? OR SECTION? OR HALF? OR FRAC-
               TION?)(2N)(TEXT OR DATA OR PLAINTEXT? OR IMAGE? OR DIGITAL()(-
               GOOD? OR DOCUMENT? OR OBJECT? OR MEDIA?) OR MULTIMEDIA OR VID-
               EO OR STREAM)
S4           0   S1(S)(S2 OR S3)(S)S4
S5          94   S1(S)(S2 OR S3)
S6          31   S5(S)(HASH OR HASHES OR HASHING OR HASHED OR CRYPTOG? OR E-
               NRYPT? OR ENCIPHER? OR DES)
S7          15   S6 NOT AD=20000830:20020830
S8          15   S7 NOT AD=20020830:20040501
File 348:EUROPEAN PATENTS 1978-2004/Apr W02
         (c) 2004 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20040415,UT=20040408
         (c) 2004 WIPO/Univentio
```

8/5,K/13 (Item 5 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00410490 **Image available**

METHODS FOR GENERATING VARIABLE S-BOXES FROM ARBITRARY KEYS OF ARBITRARY LENGTH

PROCEDES POUR GENERER DES ZONES DE SUBSTITUTION VARIABLES A PARTIR DE TOUCHES ARBITRAIRES DE LONGUEUR ARBITRAIRE

Patent Applicant/Assignee:
TELEDYNE INDUSTRIES INC,
Inventor(s):
GARCKEN Knute T,
STRAWBRIDGE Charles E,
KISYLIA Andrew Philip,

Patent and Priority Information (Country, Number, Date):
Patent: WO 9800949 A1 19980108
Application: WO 97US13624 19970627 (PCT/WO US9713624)
Priority Application: US 96673437 19960628
Designated States: CN IL JP SG AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: H04L-009/06
International Patent Class: H04L-09:28
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 11383

English Abstract
A system for generating variable substitution boxes from arbitrary keys for use in a block cipher system utilizes an initial set of linearly independent numbers (13) to generate substitution tables (15). The initial set of linearly independent numbers (13) is modulated with the bits of an arbitrary key through operations that result in final sets of linearly independent numbers to form the substitution tables (15). The system also includes an implementation which allows for rapid key changes for the crypto system by only generating portions of the substitution tables as needed for specific blocks of input data to be encrypted or decrypted.

French Abstract
L'invention concerne un systeme pour generer des zones de substitution a partir de touches arbitraires, prevu pour etre utilise dans un systeme de cryptage par codage de blocs. Ce systeme utilise un ensemble initial de nombres lineairement independants (13) pour generer des tables de substitution (15). L'ensemble initial de nombres lineairement independants (13) est module avec les bits d'une touche arbitraire par des operations qui se traduisent par des ensembles finaux de nombres lineairement independants pour former des tables de substitution (15). The systeme comprend aussi une mise en oeuvre qui permet d'effectuer des changements de touches rapides pour le systeme cryptographique en ne generant que des parties des tables de substitution requises pour des blocs specifiques de donnees d'entree devant etre codees ou decodees.

Fulltext Availability:
Detailed Description

Detailed Description
... Provide substitute values for the sub-blocks of plaintext.

Descrij;Ltion of Related Art
In **DES** , the S-Tables are organized into eight **substitution boxes** (**S - Boxes**), each of which consists of four, 16-entry S-Tables, where each S-Table entry...

...i.e., 0000 through I I I I (0 through 15). The input to a **DES S - Box** is a 6-bit sub-block. Two bits determine which of the four S-Tables

to use and the remaining four bits index the selected S-Table. In **DES**, a 56-bit key is used to generate a "schedule" of 16, 48-bit sub-keys. In each of the 16 iterations or "rounds" used by **DES**, one of the sub-keys is combined with a **portion** of the **plaintext**, or that round's derivative thereof, using an exclusive-or (XOR) operation. The 48-bit XORsum is then broken into eight, 6-bit sub-blocks and the **S - Boxes** are used to provide substitutions for those sub-blocks.

Any block cipher system may be...

8/5,K/2 (Item 2 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00866163

CONSTRUCTING SYMMETRIC CIPHERS USING THE CAST DESIGN PROCEDURE
ENTWURF SYMMETRISCHER VERSCHLUSSELUNGSVERFAHREN NACH DEM CAST-VERFAHREN
CREATION D'ALGORITHMES CRYPTOGRAPHIQUES PAR LA PROCEDURE DE CONCEPTION CAST

PATENT ASSIGNEE:
ENTRUST TECHNOLOGIES LTD., (2538870), 750 Heron Road, Tower E, Ottawa, Ontario K2G 5J9, (CA), (Proprietor designated states: all)
INVENTOR:
ADAMS, Carlisle, Michael, 1182 Soderlind Street, Ottawa, Ontario K2C 3B4, (CA)
WIENER, Michael, James, 20 Hennepin Street, Nepean, Ontario K2J 3Z4, (CA)
LOCKHART, Roland, Thomas, 27 Liston Crescent, Kanata, Ontario K2L 2W3, (CA)
LEGAL REPRESENTATIVE:
Newstead, Michael John et al (34355), Page Hargrave Southgate, Whitefriars Lewins Mead, Bristol BS1 2NT, (GB)

PATENT (CC, No, Kind, Date): EP 953244 A1 991103 (Basic)
EP 953244 B1 021023
WO 97022192 970619
APPLICATION (CC, No, Date): EP 96938884 961127; WO 96CA782 961127
PRIORITY (CC, No, Date): CA 2164768 951208
DESIGNATED STATES: CH; DE; DK; ES; FI; FR; GB; IT; LI; NL
INTERNATIONAL PATENT CLASS: H04L-009/06
CITED PATENTS (EP B): EP 618701 A; WO 91/18459 A
CITED REFERENCES (EP B):
NTT REVIEW, JULY 1994, JAPAN, vol. 6, no. 4, ISSN 0915-2334, pages 85-90, XP000460342 MIYAGUCHI S: "Secret key ciphers that change the encipherment algorithm under the control of the key"
PROCEEDINGS OF THE 3RD SYMPOSIUM ON THE STATE AND PROGRESS OF RESEARCH IN CRYPTOGRAPHY , 15 - 16 February 1993, ROME, pages 181-190, XP000617550 ADAMS ET AL.: "DESIGNING S-BOXES FOR CIPHERS RESISTANT TO DIFFERENTIAL CRYPTANALYSIS";
NOTE:
No A-document published by EPO

LEGAL STATUS (Type, Pub Date, Kind, Text):

Assignee:	000927	A1	Transfer of rights to new applicant: Nortel Networks Limited (3029040) World Trade Center of Montreal, 380 St. Antoine Street West, 8th floor Montreal, Quebec H2Y 3Y4 CA
Application:	970917	A1	International application (Art. 158(1))
Lapse:	040121	B1	Date of lapse of European Patent in a contracting state (Country, date): CH 20021023, DE 20030124, ES 20030429, FI 20021023, NL 20021023, LI 20021023,
Lapse:	031022	B1	Date of lapse of European Patent in a contracting state (Country, date): CH 20021023, FI 20021023, NL 20021023, LI 20021023,
Lapse:	030924	B1	Date of lapse of European Patent in a contracting state (Country, date): CH 20021023, NL 20021023, LI 20021023,
Grant:	021023	B1	Granted patent
Assignee:	001129	A1	Transfer of rights to new applicant: ENTRUST TECHNOLOGIES LTD. (2538870) 750 Heron Road, Tower E Ottawa, Ontario K2G 5J9 CA
Examination:	020206	A1	Date of dispatch of the first examination report: 20011221
Lapse:	030723	B1	Date of lapse of European Patent in a contracting state (Country, date): NL 20021023,
Oppn None:	031015	B1	No opposition filed: 20030724
Lapse:	040107	B1	Date of lapse of European Patent in a contracting state (Country, date): CH 20021023, DE 20030124, FI 20021023, NL

20021023, LI 20021023,
Application: 991103 A1 Published application with search report
Examination: 991103 A1 Date of request for examination: 19980910
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200243	993
CLAIMS B	(German)	200243	975
CLAIMS B	(French)	200243	1381
SPEC B	(English)	200243	5431
Total word count - document A			0
Total word count - document B			8780
Total word count - documents A + B			8780

...SPECIFICATION in data blocks of a predetermined bitlength comprising a plurality of consecutive transformation rounds of **half** of each **data** block. Each consecutive transformation round comprises steps of combining the **half** **data** block with a first masking key of predetermined length using a first binary operation to generate a first modified **half** **data** block and combining the first modified **half** **data** block with a second masking key of predetermined length using a second (different) binary operation to generate a second modified **half** **data** block. The method further includes steps of processing the second modified **half** **data** block by a plurality of (m x n) mutually different **substitution** **boxes** to generate a third modified **half** **data** block, where m and n are positive integers and m<n, and XORing the third modified **half** **data** block with the remaining **half** of the **data** block to generate a transformed **half** **data** block of a transformation round.

Brief Description of the Drawings

Figure 1 is a known...

...CLAIMS round function means has a first plurality of partially bent-function-based (m x n) **s - boxes** for processing key bits to generate a first masking key and a second masking key, and a second plurality of partially bent-function-based (m x n) **s - boxes** for processing the second modified **data** **half** .

8. The **data** encryption method of **cryptographically** transforming plaintext into ciphertext in data blocks of predetermined bitlength according to claim 6, wherein...

...round function means has a first plurality of partially bent-function-based (m x n) **s - boxes** for processing key bits to generate a first masking key and a second masking key, and a second plurality of partially bent-function-based (m x n) **s - boxes** for proccssing the second modified **data** **half** .

9. The **data** encryption method of **cryptographically** transforming plaintext into ciphertext in data blocks of predetermined bitlength according to claim 8, wherein the first plurality of **s - boxes** comprises four partially bent-function-based 8x32 **s - boxes** and the second plurality of **s - boxes** comprises four partially bent-function-based 8x32 **s - boxes** .

10. The data encryption method of cryptographically transforming plaintext into ciphertext in data blocks of...

...addition modulo 2n), subtraction modulo 2n), and bitwise XOR can be used to combine the **half** **data** block with the first masking key and to combine the **s - box** outputs which result from the processing of the second modified **half** **data** block.

14. The data encryption method of cryptographically transforming plaintext into ciphertext in data blocks...

```
Set     Items   Description
S1       5806   SBOX? OR (SUBSTITUTION? OR S)()(BOX OR BOXES)
S2    1935374   BREAK? OR DIVID? OR SPLIT? OR SUBDIVID?
S3    5087443   TEXT? OR DATA OR PLAINTEXT? OR PLAIN()TEXT? OR IMAGE? OR D-
              IGITAL()(GOOD? OR DOCUMENT? OR OBJECT? OR MEDIA?) OR MULTIMED-
              IA? OR VIDEO? OR STREAM?
S4    6626635   PORTION? OR PART? OR SECTOR? OR SECTION? OR HALF? OR FRACT-
              ION?
S5      67250   SCRAMBL? OR HASH?
S6    1355835   TABLE? OR MATRIX? OR MATRICE? OR INDEX? OR INDICE?
S7         35   S1 AND S2(2N)S3
S8        169   S1 AND S3(2N)S4
S9          2   S1(S)S2(2N)S3
S10        10   S1(S)S3(2N)S4
S11         5   S1(S)S2(S)S3(S)S4(S)(S5 OR S6)
S12        48   S7 OR S9 OR S11 OR S10
S13        41   RD (unique items)
S14        29   S13 NOT PY>2000
S15        29   S14 NOT PD=20000830:20020830
S16        29   S15 NOT PD=20020830:20040422
File 275:Gale Group Computer DB(TM) 1983-2004/Apr 19
         (c) 2004 The Gale Group
File 647:CMP  Computer Fulltext 1988-2004/Apr W2
         (c) 2004 CMP Media, LLC
File 675:TRADEMARKSCAN(R)-Sweden 2004/Apr W1
         (c) 2004 Compu-Mark N.V.
File 148:Gale Group Trade & Industry DB 1976-2004/Apr 19
         (c)2004 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2004/Apr 16
         (c) 2004 The Gale Group
```

16/3,K/13 (Item 2 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

11844967 SUPPLIER NUMBER: 60019178 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Joint Development of Next-Generation Encryption Algorithm 'Camellia' by NTT and Mitsubishi Electric.
Business Wire, 0529
March 10, 2000
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 1190 LINE COUNT: 00104

... boxes) are designed to be suitable for small hardware. The key schedule can share a **part** of **data** randomizing and the memory requirement for subkeys is reduced. As a result, Camellia encryption hardware...

```
Set     Items   Description
S1       1426   SBOX? OR (SUBSTITUTION? OR S)()(BOX OR BOXES)
S2    1617007   BREAK? OR DIVID? OR SPLIT? OR SUBDIVID?
S3    8715329   TEXT? OR DATA OR PLAINTEXT? OR PLAIN()TEXT? OR IMAGE? OR D-
             IGITAL()(GOOD? OR DOCUMENT? OR OBJECT? OR MEDIA?) OR MULTIMED-
             IA? OR VIDEO? OR STREAM?
S4   10565210   PORTION? OR PART? OR SECTOR? OR SECTION? OR HALF? OR FRACT-
             ION?
S5      37201   SCRAMBL? OR HASH?
S6    2955377   TABLE? OR MATRIX? OR MATRICE? OR INDEX? OR INDICE?
S7          6   S1 AND S2(2N)S3
S8          6   S1 AND S3(2N)S4
S9          0   S1 AND S2 AND S3 AND S5
S10         4   S1 AND S2 AND S3 AND S4
S11         5   S1 AND S2 AND S3 AND S6
S12        35   S1 AND (S2 OR S4) AND (S5 OR S6)
S13        48   S7 OR S8 OR S10 OR S11 OR S12
S14        38   RD (unique items)
S15        30   S14 NOT PY>2000
S16        30   S15 NOT PD=20000830:20020830
S17        30   S16 NOT PD=20020830:20040501
File   8:Ei Compendex(R) 1970-2004/Apr W2
         (c) 2004 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2004/Mar
         (c) 2004 ProQuest Info&Learning
File  65:Inside Conferences 1993-2004/Apr W2
         (c) 2004 BLDSC all rts. reserv.
File   2:INSPEC 1969-2004/Apr W2
         (c) 2004 Institution of Electrical Engineers
File  94:JICST-EPlus 1985-2004/Apr W1
         (c)2004 Japan Science and Tech Corp(JST)
File 111:TGG Natl.Newspaper Index(SM) 1979-2004/Apr 19
         (c) 2004 The Gale Group
File 233:Internet & Personal Comp. Abs. 1981-2003/Sep
         (c) 2003 EBSCO Pub.
File 144:Pascal 1973-2004/Apr W2
         (c) 2004 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  34:SciSearch(R) Cited Ref Sci 1990-2004/Apr W2
         (c) 2004 Inst for Sci Info
File  62:SPIN(R) 1975-2004/Feb W5
         (c) 2004 American Institute of Physics
File  99:Wilson Appl. Sci & Tech Abs 1983-2004/Mar
         (c) 2004 The HW Wilson Co.
File  95:TEME-Technology & Management 1989-2004/Mar W4
         (c) 2004 FIZ TECHNIK
```

17/5/2 (Item 2 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

04623386 E.I. No: EIP97023519318
Title: Improved Data Encryption Standard (DES) algorithm
Author: Han, Seung-Jo; Oh, Heang-Soo; Park, Jongan
Corporate Source: Chosun Univ, Kwangju, South Korea
Conference Title: Proceedings of the 1996 4th International Symposium on Spread Spectrum Techniques & Applications
Conference Location: Mainz, Ger Conference Date: 19960922-19960925
E.I. Conference No.: 45960
Source: IEEE International Symposium on Spread Spectrum Techniques & Applications v 3 1996.. p 1310-1314
Publication Year: 1996
CODEN: 85QWA7
Language: English
Document Type: CA; (Conference Article) Treatment: G; (General Review); T; (Theoretical)
Journal Announcement: 9704W1
Abstract: The cryptosystem which is most used throughout the world for protecting information is the Data Encryption Standard (DES) which was announced by National Bureau of Standard (NBS). The DES must be stronger than the other cryptosystems in the security. But, because the process time required for cryptanalysis has lessened, because hardware technique has developed rapidly, the DES may be attacked by various kinds of cryptanalysis using parallel process. It may be especially vulnerable to attack by the differential cryptanalysis. Therefore, the DES will require strengthening to ensure cryptographic security in the days to come. This paper proposes design of a DES-like cryptosystem called the Improved-DES. The Improved-DES is a new algorithm. We show that the Improved-DES is stronger than the DES against differential cryptanalysis for cryptographic security. We will **divide** one **data** block (96 bits) into 3 sub-blocks of 32 bits and then perform different f functions on each of the 3 sub-blocks, and then increase the S//1-S//8 of the **S - boxes** to S//1-S//1//6, satisfying the Strict Avalanche Criterion (SAC: p//i//j) and the correlation coefficient (p//i//j). Finally we will increase the key length to 112 bits. The analysis will show that the unicity distance (UD) in the Improved-DES is increased more than the DES's UD. (Author abstract) 13 Refs.
Descriptors: *Data communication systems; Cryptography; Standards; Security of data; Computer hardware; Correlation methods; Algorithms; Binary codes
Identifiers: Data encryption standard (DES); Strict avalanche criterion (SAC)
Classification Codes:
902.2 (Codes & Standards); 723.2 (Data Processing); 716.1 (Information & Communication Theory)
716 (Radar, Radio & TV Electronic Equipment); 723 (Computer Software); 902 (Engineering Graphics & Standards); 722 (Computer Hardware)
71 (ELECTRONICS & COMMUNICATIONS); 72 (COMPUTERS & DATA PROCESSING); 90 (GENERAL ENGINEERING)

17/5/16 (Item 6 from file: 2)
DIALOG(R)File 2:INSPEC

4923277 INSPEC Abstract Number: B9505-6120B-139, C9505-1260-114
Title: Pitfalls in designing substitution boxes
Author(s): Seberry, J.; Xian-Mo Zhang; Yuliang Zheng
Author Affiliation: Dept. of Comput. Sci., Wollongong Univ., NSW, Australia
p.383-96
Editor(s): Desmedt, Y.G.
Publisher: Springer-Verlag, Berlin, Germany
Publication Date: 1994 Country of Publication: West Germany vi+438 pp.
ISBN: 3 540 58333 5
Conference Title: Advances in Cryptology - CRYPTO '94. 14th International Cryptology Conference Proceedings
Conference Sponsor: Int. Assoc. Cryptologic Res.; IEEE Comput. Soc. Tech. Committe on Security & Privacy
Conference Date: 21-25 Aug. 1994 Conference Location: Santa Barbara, CA, USA
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: Two significant recent advances in cryptanalysis, namely the differential attack put forward by Biham and Shamir (1991) and the linear attack by Matsui (1994) have had devastating impact on data encryption algorithms. An eminent problem that researchers are facing is to design **S - boxes** or **substitution boxes** so that an encryption algorithm that employs the **S - boxes** is immune to the attacks. We present evidence indicating that there are many pitfalls on the road to achieve the goal. In **particular** , we show that certain types of **S - boxes** which are seemly very appealing do not exist. We also show that, contrary to previous perception, techniques such as chopping or repeating permutations do not yield cryptographically strong **S - boxes** . In addition, we reveal an important combinatorial structure associated with certain quadratic permutations, namely, the difference distribution **table** of each differentially 2-uniform quadratic permutation embodies a Hadamard **matrix** . As an application of this result, we show that chopping a differentially 2-uniform quadratic permutation results in an **S - box** that is very prone to the differential cryptanalytic attack. (17 Refs)
Subfile: B C
Descriptors: codes; cryptography; Hadamard **matrices**
Identifiers: **substitution boxes** ; cryptanalysis; differential attack; linear attack; data encryption algorithms; **S - boxes** ; cryptographically strong **S - boxes** ; combinatorial structure; quadratic permutations; difference distribution **table** ; differentially 2-uniform quadratic permutation; Hadamard **matrix**
Class Codes: B6120B (Codes); B6110 (Information theory); C1260 (Information theory); C6130S (Data security)

```
Set      Items    Description
S1         196    SBOX? OR (SUBSTITUTION? OR S)()(BOX OR BOXES)
S2     1017363    BREAK? OR DIVID? OR SPLIT? OR SUBDIVID?
S3     3262672    TEXT? OR DATA OR PLAINTEXT? OR IMAGE? OR DIGITAL()(GOOD? OR
                 OBJECT? OR MEDIA?) OR MULTIMEDIA? OR VIDEO? OR STREAM?
S4     7544720    PORTION? OR PART? OR SECTOR? OR SECTION? OR HALF? OR FRACT-
                 ION?
S5       11167    SCRAMBL? OR HASH?
S6      741703    TABLE? OR MATRIX? OR MATRICE? OR INDEX? OR INDICE?
S7           3    S1 AND S2(2N)S3
S8          11    S1 AND S3(2N)S4
S9          29    S2 AND S3 AND S4 AND S5 AND S6
S10         42    S7 OR S8 OR S9
S11         34    S10 NOT AD=20000830:20020830
S12         34    S11 NOT AD=2002083:20040501
S13         34    IDPAT (sorted in duplicate/non-duplicate order)
S14         33    IDPAT (primary/non-duplicate records only)
File 347:JAPIO Nov 1976-2003/Dec(Updated 040402)
         (c) 2004 JPO & JAPIO
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200425
         (c) 2004  Thomson Derwent
```

14/5/2 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014403897 **Image available**
WPI Acc No: 2002-224600/200228
Related WPI Acc No: 2000-105416
XRPX Acc No: N02-172065

Digital stream **signing method and system with reduced computation time for authentication,** divides **a** data stream **into blocks and adds ancillary information for authenticating the subsequent blocks and verifies a single digital signature**

Patent Assignee: INT BUSINESS MACHINES CORP (IBMC)
Inventor: GENNARO R; ROHATGI P
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6311271	B1	20011030	US 97799813	A	19970213	200228	B
			US 99421819	A	19991020		

Priority Applications (No Type Date): US 97799813 A 19970213; US 99421819 A 19991020
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6311271	B1		22	H04L-009/32	Cont of application US 97799813 Cont of patent US 6009176

Abstract (Basic): US 6311271 B1

NOVELTY - The original **data stream** is **partitioned** into a sequence of contiguous blocks and the software processes the original **stream** and adds ancillary information to each of the original block for authentication. The authentication information placed in the first block will be used to authenticate the following blocks. The receiver verifies the signature of the first block and subsequently verifies **hashes** of the following blocks of a single digital signature.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for a program storage device to perform the method of authentication method for a combined **stream** of **data** .

USE - Authenticating **data stream** in advance to the sender e.g. MPEG (Motion Picture Expert Group).

ADVANTAGE - This properties of the authentication information is propagated through the **stream** which reduces the computation time necessary to sign and authenticate a **stream** of **data** , by reducing the number of digital signatures required for authentication. The receiver authenticates a **stream** without receiving the entire **stream** and therefore the receiver can interrupt the transmission as soon as tampering is detected instead of receiving the whole file and then checking the signature. The size of the authentication information associated with each block does not depend on the size of the **stream** and their is no big **table** to store.

DESCRIPTION OF DRAWING(S) - The drawing shows a block diagram of a digital **stream** being **divided** into blocks and ancillary information being added for authentication.

pp; 22 DwgNo 1a/7

Title Terms: DIGITAL; **STREAM** ; SIGN; METHOD; SYSTEM; REDUCE; COMPUTATION; TIME; AUTHENTICITY; **DIVIDE** ; **DATA** ; **STREAM** ; BLOCK; ADD; ANCILLARY; INFORMATION; AUTHENTICITY; SUBSEQUENT; BLOCK; VERIFICATION; SINGLE; DIGITAL; SIGNATURE
Derwent Class: T01; W01; W04
International Patent Class (Main): H04L-009/32
File Segment: EPI

14/5/5 (Item 5 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

012267330
WPI Acc No: 1999-073436/199907
XRPX Acc No: N99-053875
Block cipher secure against differential and linear cryptanalysis - divides the input into two half-blocks which are combined with the key octet by octet, then shifted left after passing through substitution boxes
Patent Assignee: SAMSUNG ELECTRONICS CO LTD (SMSU)
Inventor: CHA Y; LEE C; CHA Y T; LEE C H
Number of Countries: 006 Number of Patents: 010
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
FR 2765056	A1	19981224	FR 987753	A	19980619	199907	B
GB 2327581	A	19990127	GB 9811900	A	19980604	199907	
DE 19827904	A1	19990114	DE 1027904	A	19980623	199908	
JP 11073101	A	19990316	JP 98175844	A	19980623	199921	
GB 2327581	B	19990804	GB 9811900	A	19980604	199933	
KR 99002840	A	19990115	KR 9726558	A	19970623	200011	
DE 19827904	C2	20000511	DE 1027904	A	19980623	200028	
JP 3148181	B2	20010319	JP 98175844	A	19980623	200125	
US 6314186	B1	20011106	US 9895845	A	19980611	200170	
KR 389902	B	20030922	KR 9726558	A	19970623	200416	

Priority Applications (No Type Date): KR 9726558 A 19970623
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
FR 2765056	A1		20	H04L-009/28	
GB 2327581	A			H04L-009/06	
DE 19827904	A1			H04L-009/06	
JP 11073101	A		8	G09C-001/00	
GB 2327581	B			H04L-009/06	
KR 99002840	A			G06F-001/00	
DE 19827904	C2			H04L-009/06	
JP 3148181	B2		11	G09C-001/00	Previous Publ. patent JP 11073101
US 6314186	B1			H04L-009/28	
KR 389902	B			G06F-001/00	Previous Publ. patent KR 99002840

Abstract (Basic): FR 2765056 A
The encryption algorithm **divides** the **data stream** into blocks of 2 N octets, and the blocks are divided into a first and a second half. An exclusive-OR operation is performed between the second half and a rotation key of M octets. The result of this step is divided into L blocks of eight bits, and the first block is sent to a first **S box**, and each of the remaining blocks sent to a corresponding **S - box** after it has been combined with the output of the preceding **S - box**.
The output of each of the **S - boxes** is rotated left, and the results used to form a new second half of the input block, while the old second half forms a new half.
USE - USE - Encryption of digital audio streams
ADVANTAGE - ADVANTAGE - Allows construction of encryption algorithm from blocks of fast algorithms to give fast encryption and decryption with algorithm that is resistant to differential and linear cryptanalysis.
Dwg.0/3
Title Terms: BLOCK; CIPHER; SECURE; DIFFERENTIAL; LINEAR; DIVIDE; INPUT; TWO; HALF; BLOCK; COMBINATION; KEY; SHIFT; LEFT; AFTER; PASS; THROUGH; SUBSTITUTE; BOX
Index Terms/Additional Words: DIGITAL; AUDIO; SIGNALS
Derwent Class: P85; T01; U21; W01
International Patent Class (Main): G06F-001/00; G09C-001/00; H04L-009/06; H04L-009/28
International Patent Class (Additional): G06F-007/38; G06F-017/10; H03K-019/20
File Segment: EPI; EngPI

14/5/7 (Item 7 from file: 350)
DIALOG(R)File 350:Derwent WPIX

011854577 **Image available**
WPI Acc No: 1998-271487/199824
XRPX Acc No: N98-213239
Data encryption method for digital data processing - expanding and processing half **a** data **block giving modified** half data **block which is XORed with remaining** half **of** data **block giving transformed** half data **block**
Patent Assignee: NORTHERN TELECOM LTD (NELE)
Inventor: LEECH M D
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5745577	A	19980428	US 96687303	A	19960725	199824	B

Priority Applications (No Type Date): US 96687303 A 19960725
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5745577	A		22	H04L-009/28	

Abstract (Basic): US 5745577 A

The method is for cryptographically transforming between plaintext and ciphertext in data blocks of a predetermined bitlength in which the data blocks are processed sequentially through a number of transformation round. Each round includes

expanding a **half** of a **data** block and XORing it with a subkey to generate a modified **half data** block.

The modified **half data** block is processed by two or more sets of a number of different **substitution boxes** to generate a second modified **half data** block. The second modified **half data** block is then XORed with the remaining **half** of the **data** block to generate a transformed **half data** block of a transformation round.

ADVANTAGE - The method is immune to differential and linear cryptanalysis and provides an internal key scheduling mechanism which generates no weak or semi-weak encryption keys

Dwg.5/13

Title Terms: DATA; ENCRYPTION; METHOD; DIGITAL; DATA; PROCESS; EXPAND; PROCESS; HALF; DATA; BLOCK; MODIFIED; HALF; DATA; BLOCK; REMAINING; HALF; DATA; BLOCK; TRANSFORM; HALF; DATA; BLOCK
Derwent Class: W01
International Patent Class (Main): H04L-009/28
International Patent Class (Additional): H04L-009/00; H04L-009/06
File Segment: EPI

14/5/8 (Item 8 from file: 350)
DIALOG(R)File 350:Derwent WPIX

011355167 **Image available**
WPI Acc No: 1997-333074/199730
XRPX Acc No: N97-276426

Symmetric encryption family algorithm design procedure especially for CAST ciphers - using several consecutive transformation rounds of half **of each** data **block combining each half block with masking key using binary operations and combining them to for cipher**

Patent Assignee: ADAMS C M (ADAM-I); ENTRUST TECHNOLOGIES LTD (ENTR-N); NORTEL NETWORKS CORP (NELE); NORTHERN TELECOM LTD (NELE)
Inventor: ADAMS C M; LOCKHART R T; WIENER M J
Number of Countries: 021 Number of Patents: 008
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9722192	A1	19970619	WO 96CA782	A	19961127	199730	B
CA 2164768	A	19970609	CA 2164768	A	19951208	199741	
US 5825886	A	19981020	US 96761763	A	19961205	199849	
EP 953244	A1	19991103	EP 96938884	A	19961127	199951	
			WO 96CA782	A	19961127		
JP 2000506620	W	20000530	WO 96CA782	A	19961127	200033	
			JP 97521561	A	19961127		
CA 2164768	C	20010123	CA 2164768	A	19951208	200108	
EP 953244	B1	20021023	EP 96938884	A	19961127	200277	
			WO 96CA782	A	19961127		
DE 69624514	E	20021128	DE 624514	A	19961127	200303	
			EP 96938884	A	19961127		
			WO 96CA782	A	19961127		

Priority Applications (No Type Date): CA 2164768 A 19951208
Cited Patents: 2.Jnl.Ref; EP 618701; WO 9118459
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9722192	A1	E	38	H04L-009/06	
Designated States (National): JP					
Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE					
CA 2164768	A			G09C-001/00	
US 5825886	A			H04L-009/28	
EP 953244	A1	E			Based on patent WO 9722192
Designated States (Regional): CH DE DK ES FI FR GB IT LI NL					
JP 2000506620	W		42	G09C-001/00	Based on patent WO 9722192
CA 2164768	C	E		G09C-001/00	
EP 953244	B1	E		H04L-009/06	Based on patent WO 9722192
Designated States (Regional): CH DE DK ES FI FR GB IT LI NL					
DE 69624514	E			H04L-009/06	Based on patent EP 953244
					Based on patent WO 9722192

Abstract (Basic): WO 9722192 A

The data encryption method of cryptographically transforming plaintext into ciphertext in data blocks of a predetermined bit length includes several consecutive transformation rounds of **half** of each **data** block. Each consecutive transformation round involves combining the **half** **data** block with a first masking key of predetermined length using a first binary operation to generate a first modified **half** **data** block. The first modified **half** **data** block is combined with a second masking key of predetermined length using a second and different binary operation to generate a second modified **half** **data** block.

The second modified **half** **data** block is processed using several (m x n) mutually different **substitution** **boxes** to generate a third modified **half** **data** block, m and n being positive integer. The third modified **half** **data** block is XORed with the remaining **half** of the **data** block to generate a transformed **half** **data** block of a transformation round.

USE/ADVANTAGE - Provides resistance to differential cryptanalysis

and related key cryptanalysis.

Dwg.2/2

Title Terms: SYMMETRICAL; ENCRYPTION; FAMILY; ALGORITHM; DESIGN; PROCEDURE; CAST; CIPHER; CONSECUTIVE; TRANSFORM; ROUND; HALF; DATA; BLOCK; COMBINATION; HALF; BLOCK; MASK; KEY; BINARY; OPERATE; COMBINATION; CIPHER

Derwent Class: P85; W01

International Patent Class (Main): G09C-001/00; H04L-009/06; H04L-009/28

File Segment: EPI; EngPI

14/5/14 (Item 14 fi[redacted] file: 350)
DIALOG(R)File 350:Derwent WPIX

008534556 **Image available**
WPI Acc No: 1991-038619/199106
XRPX Acc No: N91-029817

Data enciphering system for computer - supplying successive data words to cipher circuit where each word is consecutively modified several times

Patent Assignee: TULIP COMPUTERS INT (TULI-N); TULIP COMPUTERS INT BV (TULI-N)
Inventor: KWAN B C T; VANRUMPT H W; VAN RUMPT H W
Number of Countries: 010 Number of Patents: 005
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 411712	A	19910206	EP 90202092	A	19900731	199106	B
NL 8901983	A	19910301				199113	
US 5231662	A	19930727	US 90560144	A	19900731	199331	
			US 91794326	A	19911112		
EP 411712	B1	19961002	EP 90202092	A	19900731	199644	
DE 69028748	E	19961107	DE 628748	A	19900731	199650	
			EP 90202092	A	19900731		

Priority Applications (No Type Date): NL 891983 A 19890801
Cited Patents: 1.Jnl.Ref; EP 114368; US 4278837; US 4780905
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5231662	A		7	H04L-009/06	Cont of application US 90560144
EP 411712	B1	E	12	H04L-009/06	
Designated States (Regional): BE DE DK ES FR GB IT NL SE					
DE 69028748	E			H04L-009/06	Based on patent EP 411712

Abstract (Basic): EP 411712 A

The system enciphers all data words of e.g. 16 bits to be stored into a computer using a product cipher circuit includes alternately one from several permutation boxes (1-1 to 1-11) and one from a number of **substitution boxes** (1-12 to 1-51) each box being under the control of a specific part of a key.

The data words are enciphered in whole and the system can be regarded as a delay line. The data words can be combined with storage sector-specific coding words and with a key entered on an input device (2).

ADVANTAGE - Does not cause any delay that is noticeable to user.

(8pp Dwg.No.1/1

Title Terms: DATA; ENCIPHER; SYSTEM; COMPUTER; SUPPLY; SUCCESSION; DATA; WORD; CIPHER; CIRCUIT; WORD; CONSECUTIVE; MODIFIED; TIME
Derwent Class: T01; U21; W01
International Patent Class (Main): H04L-009/06
International Patent Class (Additional): G06F-012/14
File Segment: EPI

14/5/22 (Item 22 from file: 347)
DIALOG(R)File 347:JAPIO

06083044 **Image available**
CIPHERING DEVICE

PUB. NO.: 11-024558 [JP 11024558 A]
PUBLISHED: January 29, 1999 (19990129)
INVENTOR(s): KANDA MASASUKI
TAKASHIMA YOICHI
AOKI KATSUHIKO
MATSUMOTO TSUTOMU
APPLICANT(s): NIPPON TELEGR & TELEPH CORP <NTT>
N T T ELECTRON KK
APPL. NO.: 09-173671 [JP 97173671]
FILED: June 30, 1997 (19970630)
INTL CLASS: G09C-001/00; H04L-009/06

ABSTRACT

PROBLEM TO BE SOLVED: To increase the safety of a difference deciphering method and a linear deciphering method.

SOLUTION: Similarly to the conventional DES(data encryption standard), input **data** is **divided** into two **partial data** R and L and the data R is nonlinearly converted by a nonlinear function means 304 with key data; and its output and the other **partial data** of the L are exclusively ORed and the array of the output and **partial data** R is converted into the data R and L, the same process is repeated and the input data are linearly converted 341 with key data in this case as a means 304 and the output is divided into bits in0 and in1; and one of function structures 3430, 3431...3437 which are mutually and nonlinearly converted through three nonlinear means similar to one element **S - box** and three exclusive OR operations and in0 and in1 are inputted to the selected structure, whose outputs out0 and out1 are subjected to bit combination to obtain the output of the means 304.

Pitfalls in Designing Substitution Boxes (Extended Abstract)

Jennifer Seberry, Xian-Mo Zhang and Yuliang Zheng

Department of Computer Science
University of Wollongong, Wollongong, NSW 2522, Australia
{jennie, xianmo, yuliang}@cs.uow.edu.au

Abstract. Two significant recent advances in cryptanalysis, namely the differential attack put forward by Biham and Shamir [3] and the linear attack by Matsui [7, 8], have had devastating impact on data encryption algorithms. An eminent problem that researchers are facing is to design S-boxes or substitution boxes so that an encryption algorithm that employs the S-boxes is immune to the attacks. In this paper we present evidence indicating that there are many pitfalls on the road to achieve the goal. In particular, we show that certain types of S-boxes which are seemly very appealing do not exist. We also show that, contrary to previous perception, techniques such as chopping or repeating permutations do *not* yield cryptographically strong S-boxes. In addition, we reveal an important combinatorial structure associated with certain quadratic permutations, namely, the difference distribution table of each differentially 2-uniform quadratic permutation embodies a Hadamard matrix. As an application of this result, we show that chopping a differentially 2-uniform quadratic permutation results in an S-box that is very prone to the differential cryptanalytic attack.

1 Basic Definitions

Denote by V_n the vector space of n tuples of elements from $GF(2)$. Let $\alpha = (a_1, \ldots, a_n)$ and $\beta = (b_1, \ldots, b_n)$ be two vectors in V_n. The scalar product of α and β, denoted by $\langle \alpha, \beta \rangle$, is defined by $\langle \alpha, \beta \rangle = a_1 b_1 \oplus \cdots \oplus a_n b_n$, where multiplication and addition are over $GF(2)$. In this paper we consider Boolean functions from V_n to $GF(2)$ (or simply functions on V_n).

Let f be a function on V_n. The $(1, -1)$-sequence defined by $((-1)^{f(\alpha_0)}, (-1)^{f(\alpha_1)}, \ldots, (-1)^{f(\alpha_{2^n-1})})$ is called the *sequence* of f, and the $(0, 1)$-sequence defined by $(f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{2^n-1}))$ is called the *truth table* of f, where $\alpha_0 = (0, \ldots, 0, 0)$, $\alpha_1 = (0, \ldots, 0, 1)$, $\ldots$, $\alpha_{2^n-1} = (1, \ldots, 1, 1)$. f is said to be *balanced* if its truth table has 2^{n-1} zeros (ones).

An *affine* function f on V_n is a function that takes the form of $f = a_1 x_1 \oplus \cdots \oplus a_n x_n \oplus c$, where $a_j, c \in GF(2)$, $j = 1, 2, \ldots, n$. Furthermore f is called a *linear* function if $c = 0$. The sequence of an affine (or linear) function is called an *affine (or linear) sequence*.

The *Hamming weight* of a vector $\alpha \in V_n$, denoted by $W(\alpha)$, is the number of ones in the vector.

Y.G. Desmedt (Ed.): Advances in Cryptology - CRYPTO '94, LNCS 839, pp. 383-396, 1994.

A $(1,-1)$-matrix H of order m is called a *Hadamard* matrix if $HH^t = mI_m$, where H^t is the transpose of H and I_m is the identity matrix of order m. A *Sylvester-Hadamard matrix* or *Walsh-Hadamard matrix* of order 2^n, denoted by H_n, is generated by the following recursive relation

$$H_0 = 1,\ H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix},\ n = 1, 2, \ldots.$$

Now we introduce bent functions, an important combinatorial concept discovered by Rothaus in the mid 1960's, although his pioneering work was not published until some ten years later [14].

Definition 1. A function f on V_n is said to be bent if

$$2^{-\frac{n}{2}} \sum_{x \in V_n} (-1)^{f(x) \oplus \langle \beta, x \rangle} = \pm 1$$

for every $\beta \in V_n$. Here $x = (x_1, \ldots, x_n)$ and $f(x) \oplus \langle \beta, x \rangle$ is considered as a real valued function.

Bent functions can be characterized in various ways. In particular, the following statements are equivalent (see also [6]):

(i) f is bent.
(ii) $\langle \xi, \ell \rangle = \pm 2^{\frac{1}{2}n}$ for any affine sequence ℓ of length 2^n, where ξ is the sequence of f.
(iii) $f(x) \oplus f(x \oplus \alpha)$ is balanced for any non-zero vector $\alpha \in V_n$, where $x = (x_1, \ldots, x_n)$.

An $n \times s$ S-box or substitution box is a mapping from V_n to V_s, where $n \geq s$. Now we consider a nonlinearity criterion that measures the strength of an S-box against differential cryptanalysis [3, 4]. The essence of a differential attack is that it exploits particular entries in the difference distribution tables of S-boxes employed by a block cipher. The difference distribution table of an $n \times s$ S-box is a $2^n \times 2^s$ matrix. The rows of the matrix, indexed by the vectors in V_n, represent the change in the input, while the columns, indexed by the vectors in V_s, represent the change in the output of the S-box. An entry in the table indexed by (α, β) indicates the number of input vectors which, when changed by α (in the sense of bit-wise XOR), result in a change in the output by β (also in the sense of bit-wise XOR).

Note that an entry in a difference distribution table can only take an even value, the sum of the values in a row is always 2^n, and the first row is always $(2^n, 0, \ldots, 0)$. As entries with higher values in the table are particularly useful to differential cryptanalysis, a necessary condition for an S-box to be immune to differential cryptanalysis is that it does not have large values in its differential distribution table (not counting the first entry in the first row).

Definition 2. Let F be an $n \times s$ S-box, where $n \geq s$. Let δ be the largest value in differential distribution table of the S-box (not counting the first entry in the first row), namely,

$$\delta = \max_{\alpha \in V_n, \alpha \neq 0} \max_{\beta \in V_s} |\{x | F(x) \oplus F(x \oplus \alpha) = \beta\}|.$$

Then F is said to be *differentially δ-uniform*, and accordingly, δ is called the differential uniformity of f.

Obviously the differential uniformity δ of an $n \times s$ S-box is constrained by $2^{n-s} \leq \delta \leq 2^n$. Extensive research has been carried out in constructing differentially δ-uniform S-boxes with a low δ [1, 13, 2, 9, 10, 11, 12]. Some constructions, in particular those based on permutation polynomials on finite fields, are simple and elegant. However, caution must be taken with Definition 2. In particular, it should be noted that low differential uniformity (a small δ) is only a *necessary*, but not a *sufficient* condition for immunity to differential attacks. This is shown by the fact that S-boxes constructed in [1, 9], which have a flat difference distribution table, are extremely weak to differential attacks, despite that they achieve the lowest possible differential uniformity $\delta = 2^{n-s}$ [4, 5, 15]. A more complete measurement that takes into account the number of nonzero entries in the first column of a difference distribution table is the *robustness* introduced in [15].

Definition 3. Let $F = (f_1, \ldots, f_s)$ be an $n \times s$ S-box, where f_i is a function on V_n, $i = 1, \ldots, s$, and $n \geq s$. Denote by L the largest value in the difference distribution table of F, and by N the number of nonzero entries in the first column of the table. In either case the value 2^n in the first row is not counted. Then we say that F is R-robust against differential cryptanalysis, where R is defined by

$$R = (1 - \frac{N}{2^n})(1 - \frac{L}{2^n}).$$

Robustness gives more accurate information about the strength of an S-box against the differential attack than differential uniformity does. However, differential uniformity has an advantage over robustness in that the former is easier to discuss than the latter. For this reason, differential uniformity is employed as the first indicator for the strength of an S-box against the differential attack, while robustness is considered when more complete information about the strength is needed.

An $n \times s$ S-box $F = (f_1, \ldots, f_s)$ is said to be *regular* if F runs through each vector in V_s 2^{n-s} times while x runs through V_n once. S-boxes employed by a block cipher must be regular, since otherwise the cipher would be prone to statistical attacks. For a regular $n \times s$ S-box, its differential uniformity is larger than 2^{n-s} (see also Lemma 2 of [17]). The robustness of the S-box is further determined by the number of nonzero entries in the first column of the table.

We are particularly interested in $n \times s$ S-boxes that have the following property: for any nonzero vector $\alpha \in V_n$, $F(x) \oplus F(x \oplus \alpha)$ runs through half of the

vectors in V_s, each 2^{n-s+1} times, but not through the other half of the vectors in V_n. With each row in the difference distribution table of such an S-box, half of its entries contain a value 2^{n-s+1} while the other half contain a value zero. For simplicity, we say such a difference distribution table to be ***uniformly half-occupied***. Clearly an $n \times s$ S-box with a UHODDT or uniformly half-occupied difference distribution table achieves the differential uniformity of 2^{n-s+1}. In Theorem 3 of [17], it has been proved that for quadratic S-boxes, 2^{n-s+1} is the lower bound on differential uniformity.

Note that a differentially 2-uniform permutation is also a permutation with a UHODDT, and vice versa. These permutations have many nice properties [13, 2, 9, 10, 11, 12]. In particular, they achieve the highest possible robustness against the differential attack. The concept of $n \times s$ S-boxes with a UHODDT can be viewed as a generalization of differentially 2-uniform permutations. Hence $n \times s$ S-boxes with a UHODDT are very appealing and have received extensive research (see for instance [2]).

There are two important questions about S-boxes with a UHODDT, namely

(i) Do there exist S-boxes with a UHODDT ? If there do, how to construct them ?
(ii) What is the robustness of an S-box with a UHODDT ?

When $n = s$, the answer to the first question is "yes". It has been shown in [13, 11, 2] that certain permutation polynomials on $GF(2^n)$, n odd, have a UHODDT. So far no result has been known regarding the case of $n > s$. In Section 2, we will partially solve the problem by showing that there exist no quadratic $n \times s$ S-boxes with a UHODDT, if either n or s is even. The second question will be discussed in Section 3. We will prove that the robustness of an S-box with a UHODDT is very low.

Another important question is the synthesis of S-boxes, namely

(iii) How to construct S-boxes from existing ones ?

This question will be discussed in Section 4. We will show that many synthesis methods *which were previously taken for granted*, in fact do *not* yield strong S-boxes, even though the starting S-boxes employed are all strong ones. Section 5 is solely devoted to the investigation of combinatorial properties of the differential distribution table of an quadratic permutation. We reveal a result that is very interesting even from the point of view of pure combinatorics, namely, every uniformly half-occupied difference distribution table of a quadratic permutation embodies a Sylvester-Hadamard matrix.

2 Nonexistence of Certain Quadratic S-boxes

2.1 On Quadratic S-boxes with a UHODDT

As mentioned in the previous section, an $n \times s$ S-box with a UHODDT or uniformly half-occupied difference distribution table achieves the differential uniformity of 2^{n-s+1}, and for quadratic S-boxes, 2^{n-s+1} is the lower bound on

differential uniformity. In the following we show an impossibility result, namely, there exist no quadratic S-boxes that have a UHODDT if either n or s is even.

Assume that $F = (f_1, \ldots, f_s)$ is a quadratic $n \times s$ S-box with a UHODDT, where $n > s$. We prove that neither n nor s can be even.

Recall that a vector $\alpha \in V_n$ is called a *linear structure* of a function f on V_n if $f(x) \oplus f(x \oplus \alpha)$ is a constant. The set of the linear structures of f forms a linear subspace. The dimension of the subspace is called the *linearity dimension* of f. Let $\alpha_1, \ldots, \alpha_{2^n-1}$ be the $2^n - 1$ nonzero vectors in V_n and $g_1, \ldots, g_{2^s-1}$ be the $2^s - 1$ nonzero linear combinations of $f_1, \ldots, f_s$. We construct a bipartite graph whose vertices comprise $\alpha_1, \ldots, \alpha_{2^n-1}$ on one side and $g_1, \ldots, g_{2^s-1}$ on the other side. An edge or link between α_i and g_j exists if and only if α_i is a linear structure of g_j.

Theorem 2 of [17] states that $n - \ell_i$ is even, where ℓ_i is the linearity dimension of g_i. Equivalently, n and ℓ_i must be both even or both odd. Since each g_i is balanced, it can not be bent. By Lemma 5 of [17], a quadratic function is bent if and only if it does not have linear structures. Hence we have $\ell_i \geq 1$. On the other hand, from the proof for Corollary 1 of [17], we have $\ell_i \leq n - 2$. We distinguish the following two cases:

Case 1: n is odd and ℓ_i is $1, 3, 5, \ldots$, or $n - 2$.

Case 2: n is even and ℓ_i is $2, 4, 6, \ldots$, or $n - 2$.

First we consider Case 1. Let p_j denote the number of ℓ_i, $1 \leq i \leq 2^n - 1$, such that $\ell_i = j$. Then we have a sequence of numbers $p_1, p_3, p_5, \ldots, p_{n-2}$. Obviously,

$$p_1 + p_3 + p_5 + \cdots + p_{n-2} = 2^s - 1. \tag{1}$$

Since F is a S-box with a UHODDT, for any nonzero vector $\alpha_k \in V_n$

$$F(x) \oplus F(x \oplus \alpha_k) = (f_1(x) \oplus f_1(x \oplus \alpha_k), \ldots, f_s(x) \oplus f_s(x \oplus \alpha_k))$$

is not regular. Thus, by Lemma 6, there exists a linear combination of $f_1(x) \oplus f_1(x \oplus \alpha_k), \ldots, f_s(x) \oplus f_s(x \oplus \alpha_k)$, say $g_j(x) \oplus g_j(x \oplus \alpha_k)$, such that $g_j(x) \oplus g_j(x \oplus \alpha_k)$ is not balanced. Since $g_j(x) \oplus g_j(x \oplus \alpha_k)$ is affine, $g_j(x) \oplus g_j(x \oplus \alpha_k)$ must be constant. This proves that any nonzero vector $\alpha_k \in V_n$ is a linear structure of a g_j, a linear combination of $f_1, \ldots, f_s$. On the other hand, by Theorem 4 of [17], for each α_k, there exists at most one g_j among $g_1, \ldots, g_{2^s-1}$ such that α_k is a linear structure of g_j. By the construction of the bipartite graph, each α_k is linked to a unique g_j. Also each g_i with $\ell_i = j$ has j linearly independent linear structures and $2^j - 1$ nonzero linear structures. Hence we have

$$(2^1 - 1)p_1 + (2^3 - 1)p_3 + (2^5 - 1)p_5 + \cdots + (2^{n-2} - 1)p_{n-2} = 2^n - 1. \tag{2}$$

From (1) and (2) we have

$$(2^1 - 2)p_1 + (2^3 - 2)p_3 + (2^5 - 2)p_5 + \cdots + (2^{n-2} - 2)p_{n-2} = 2^n - 2^s$$

or equivalently

$$(2^2 - 1)p_3 + (2^4 - 1)p_5 + \cdots + (2^{n-3} - 1)p_{n-2} = 2^{s-1}(2^{n-s} - 1) \tag{3}$$

Note that $2^k - 1$ is divisible by 3 if and only $k \geq 2$ is even. Thus the left hand side of (3) is divisible by 3. This implies that the $(2^{n-s} - 1)$ part in the right hand side of the equation is divisible by 3. Hence s must be odd. Thus there exists no quadratic $n \times s$ S-box with a UHODDT if n is odd ($n \geq 5$) and s is even.

We now consider Case 2. Let q_j denote the number of ℓ_i, $1 \leq i \leq 2^n - 1$, such that $\ell_i = j$. Similarly to Case 1, we have a sequence of numbers $q_2, q_4, q_6, \ldots, q_{n-2}$, and

$$q_2 + q_4 + q_6 \cdots + q_{n-2} = 2^s - 1,$$
$$(2^2 - 1)q_2 + (2^4 - 1)q_4 + (2^6 - 1)q_6 + \cdots + (2^{n-2} - 1)q_{n-2} = 2^n - 1.$$

By simple deduction,

$$(2^3 - 2)q_4 + (2^5 - 2)q_6 + \cdots + (2^{n-3} - 2)q_{n-2} = 2^{n-1} - 3 \cdot 2^{s-1} + 1. \quad (4)$$

It is not hard to see that the left hand side of (4) is even when $n \geq 4$, while the right hand side of (4) is always odd for $s \geq 2$. From this we can conclude that there exists no quadratic $n \times s$ S-box with a UHODDT if n is even with $n \geq 4$.

Summarizing Case 1 and Case 2, we have

Theorem 4. *For $n \geq 4$, there exists no quadratic $n \times s$ S-box with a UHODDT if either n or s is even.*

Theorem 4 can be viewed as an extension of Corollary 2 in [17], which states that there exists no differentially 2-uniform quadratic permutation on an even dimensional vector space.

By Theorem 4, $n \times s$ S-boxes with a UHODDT do not exist if either n or s is even. When n is odd and $n = s$, as mentioned before, we do have differentially 2-uniform quadratic permutation [13, 2, 11]. Thus a problem that is left open is whether there are quadratic S-boxes with a UHODDT for $n > s$, both n and s odd. It should be pointed out that an S-box which has an odd number of input bits and also an odd number of output bits may not be very useful in practice.

2.2 An Extension

The result in the previous subsection can be extended to a special kind of differentially 2^{n-s+t}-uniform quadratic S-boxes. Let F be a $n \times s$ S-box such that for any nonzero vector $\alpha \in V_n$, $F(x) \oplus F(x \oplus \alpha)$ runs through 2^{s-t} vectors in V_s, each 2^{n-s+t} times, but not through the remaining $2^s - 2^{s-t}$ vectors in V_s, where $t \geq 1$. The case when $t = 1$ has been discussed in the previous subsection. In the following we present a nonexistence result on the case when $t > 1$.

Theorem 5. *If n is odd and t is even, there exists no quadratic $n \times s$ S-boxes such that for any nonzero vector $\alpha \in V_n$, $F(x) \oplus F(x \oplus \alpha)$ runs through 2^{s-t} vectors in V_s, each 2^{n-s+t} times, but not through the remaining vectors in V_s.*

The proof will be provided in the full version.

3 Columns of a UHODDT

In the previous section we proved that there does not exist a quadratic $n \times s$ S-box with a UHODDT if either n or s is even. It is not clear whether or not higher degree S-boxes with a UHODDT exist. If there do exist such S-boxes, we would like to know whether or not they satisfy a more stringent requirement, namely high robustness. Results to be shown below give a negative answer to the question.

The following lemma is exactly the same as Theorem 1 of [17].

Lemma 6. *Let $F = (f_1, \ldots, f_s)$ be a mapping from V_n to V_s, where each f_j is a function on V_n. Then F is regular if and only if each nonzero linear combination of $f_1, \ldots, f_s$ is balanced.*

It is easy to show that the profile of the difference distribution table of an S-box is not changed by a nonsingular linear transformation on input coordinates (see for instance [2, 17]). In particular we have

Lemma 7. *Let $F = (f_1, \ldots, f_s)$ be a regular S-box with a UHODDT or uniformly half-occupied difference distribution table. Let A be a nonsingular matrix of order n and B a nonsingular matrix of order s over $GF(2)$. Then both Let $G(x) = F(xA) = (f_1(xA), \ldots, f_n(xA))$ and $H(x) = F(x)B = (f_1(x), \ldots, f_n(x))B$ are regular S-boxes with a UHODDT.*

By definition, each row in a uniformly half-occupied difference distribution table, except the first, contains an equal number of zero and nonzero entries. The following lemma shows that a similar result holds with columns in the table.

Lemma 8. *Let F be a regular $n \times s$ S-box with a UHODDT. Then each column, except the first, in the difference distribution table contains an equal number of zero and nonzero entries.*

Proof. We prove that for each nonzero $\beta \in V_s$, there exist 2^{n-1} nonzero $\alpha \in V_n$ such that $F(x) \oplus F(x \oplus \alpha) = \beta$ has solutions for x.

Fix $x_0 \in V_n$. Since the difference distribution table of F is uniformly half-occupied, $F(x_0) \oplus F(x_0 \oplus \alpha)$ runs through each nonzero $\beta \in V_s$ 2^{n-s} times while α runs through V_n. As x_0 is arbitrary, for each nonzero $\beta \in V_s$, there exist $2^n \cdot 2^{n-s}$ pairs (x, α) such that $F(x) \oplus F(x \oplus \alpha) = \beta$, where $\alpha \neq 0$. On the other hand, since the difference distribution table of F is uniformly half-occupied, $F(x) \oplus F(x \oplus \alpha) = \beta$ either has 2^{n-s+1} solutions or has no solution for x. Thus for each nonzero $\beta \in V_s$ there exist $2^n \cdot 2^{n-s}/2^{n-s+1} = 2^{n-1}$ nonzero vectors $\alpha \in V_n$ such that $F(x) \oplus F(x \oplus \alpha) = \beta$ has solutions for x.

Recall that the robustness of an S-box is determined by the largest value in the difference distribution table of the S-box, and also by the number of nonzero entries in the first column of the table. The lemma described below gives the precise number of nonzero entries in the first column of a uniformly half-occupied difference distribution table.

Lemma 9. *Let F be a regular $n \times s$ S-box with a UHODDT. Then there are $2^{n-1} - 2^{s-1}$ nonzero entries in the first column of the difference distribution table (excluding the first entry).*

As an immediate consequence of Lemma 9, we obtain the robustness of an S-box with a UHODDT:

$$R = [1 - (2^{n-1} - 2^{s-1})/2^n](1 - 2^{n-s+1}/2^n) = (1/2 + 2^{-n+s-1})(1 - 2^{-s+1}).$$

When $n = s$, we have $R = 1 - 2^{-n+1}$, which is the highest possible value for robustness. However, when s is relatively smaller than n, say $n - s > 3$, R is very close to $1/2$. For comparison, we note that the robustness of S-boxes constructed in [15] is at least $7/8$.

4 On Methods for Synthesizing S-boxes

This section is concerned with methods for constructing S-boxes from existing ones. We show that a number of techniques which were previously taken for granted do not yield good S-boxes.

4.1 Chopping Permutations

Chopping permutations which are cryptographically strong has been conceived as a promising method to construct S-boxes for DES-like encryption algorithms. For this reason, many researchers have focused their attention on permutations, especially those on a finite field [2, 9, 10, 11, 12]. Results to be present in this subsection indicate that, contrary to the common perception, this practice does not produce good S-boxes.

First we prove the following:

Theorem 10. *Let $F = (f_1, \ldots, f_s)$ be a regular $n \times s$ S-box with a UHODDT, where $n \geq s$ and each f_j is a function on V_n. The following two statements hold:*

(i) Let $1 \leq t \leq s-1$ and let G be an S-box obtained by dropping $s-t$ component functions from F, say $G = (f_1, \ldots, f_t)$. Then the difference distribution table of G is not uniformly half-occupied.

(ii) Let $n \geq t \geq s+1$ and let H be an S-box obtained by adding $t-s$ component functions to F, say $H = (f_1, \ldots, f_s, f_{s+1}, \ldots, f_t)$, where $f_{s+1}, \ldots, f_t$ are newly added. Then the difference distribution table of H is not uniformly half-occupied.

Proof. (i) Since F has a UHODDT, for any nonzero $\alpha \neq 0$, $F(x) \oplus F(x \oplus \alpha)$ runs through 2^{s-1} vectors in V_s, each 2^{n-s+1} times, but not through the other 2^{s-1} vectors in V_s, while α runs through V_n. Fix a nonzero vector, say $\gamma = (0, \beta) \in V_s$, where 0 is the zero vector in V_t and β is a nonzero vector in V_{s-t}. By Lemma 8 there exist 2^{n-1} nonzero vector α such that $F(x) \oplus F(x \oplus \alpha) = \gamma$ has solutions for x. Thus there exist 2^{n-1} nonzero vector α such that $G(x) \oplus G(x \oplus \alpha) = 0$, where

0 is the zero vector in V_t, has solutions for x. It is easy to show that G is not uniformly half-occupied. Since G is regular there exist $2^{n-1}-2^{t-1}$ nonzero vector α such that $G(x) \oplus G(x \oplus \alpha) = 0$ (see Lemma 8) if G is uniformly half-occupied.

(ii) follows (i).

From Theorem 10 chopping a regular S-box with a UHODDT does not yield a regular S-box with a UHODDT. In particular, chopping a differentially 2-uniform permutation on V_n does not produce an S-box with a UHODDT.

As quadratic permutations with a UHODDT or differentially 2-uniform quadratic permutations have been studied very extensively, an important problem is about the structure of the difference distribution table of an S-box obtained by chopping such a permutation. We will devote a single section, Section 5, to this topic.

In addition to chopping permutations, other techniques, such as linear transforms or modulo operations on inputs or outputs of differentially 2-uniform permutations, and repeating differentially 2-uniform permutations, are also conceived as possible S-box synthesis methods. In the following we show that none of these methods generates an S-box with a UHODDT.

4.2 Linear Transforms Applied on Inputs

Let F be a differentially 2-uniform permutation on V_s, B a matrix of order $n \times s$ $(n > s)$ over $GF(2)$. Set $G(y) = F(yB)$ where $y \in V_n$. Since the rank of B is s, yB runs through 2^s vectors in V_s each 2^{n-s} times while y runs through V_n. Since F is a permutation on V_s, $G(y)$ is a regular $n \times s$ S-box.

Unfortunately the difference distribution table of $G(y)$ is not uniformly half-occupied. The reason is described in the following. Since $n > s$ there exists a nonzero vector, say β, such that $\beta B = 0$, where 0 is the zero vector in V_s. Note that $G(y) \oplus G(y \oplus \beta) = F(yB) \oplus F((y \oplus \beta)B) = F(yB) \oplus F(yB \oplus \beta B) = F(yB) \oplus F(yB) = 0$, where 0 is the zero vector in V_s, for every $y \in V_n$.

4.3 Linear Transforms Applied on Outputs

Let F be a differentially 2-uniform permutation on V_s, and B a matrix of order $n \times s$ $(n > s)$ over $GF(2)$. Set $G(x) = F(x)B$. Note that the rank of B is s. Hence yB runs through 2^s vectors in V_s each 2^{n-s} times while y runs through V_n. As F is a permutation on V_n, G is a regular $n \times s$ S-box.

Since $n > s$, there exists a matrix of order $n \times (n-s)$, say D, such that the matrix $A = [BD]$ of order n is nonsingular. Set $\Psi(x) = F(x)A$. By Lemma 7, Ψ is a also a differentially 2-uniform permutation. By Theorem 10, G is not an S-box with a UHODDT.

4.4 Connecting Permutations in Parallel

Let F be a differentially 2-uniform permutation on V_s. Set

$$G(y) = (1 \oplus x_{s+1})F(x) \oplus x_{s+1}F(x \oplus \alpha)$$

where $x = (x_1, \ldots, x_s)$, $y = (x_1, \ldots, x_s, x_{s+1})$, $\alpha \in V_s$. Note that $G(x, 0) = F(x)$, $G(x, 1) = F(x \oplus \alpha)$. Since F is permutation on V_s G is a regular $(s+1) \times s$ S-box.

Let $\beta = (\alpha, 1)$. Clearly $G(y \oplus \beta) = G(y)$ for every $y \in V_{s+1}$. Thus $G(y) \oplus G(y \oplus \beta) = 0$, where 0 is the zero vector in V_s, for every $y \in V_n$. Thus the difference distribution is very bad in this case, and $G(y)$ is not an S-box with a UHODDT.

The above discussions can be extended to the general case where F is repeated 2^k times, $k \geq 1$.

4.5 Enlarging Inputs or Reducing Outputs by Modulo Operations

Let $\alpha = (a_1, \ldots, a_n) \in V_n$. Rewrite α as $\alpha = a_1 \oplus a_2 x \oplus \cdots \oplus a_n x^{n-1}$. Thus V_n and the set of polynomials of degree at most $n-1$ over $GF(2)$ have a one-to-one correspondence. Let $\sigma(x)$ be a primitive polynomial of degree s $(s < n)$. For any $\alpha \in V_n$, we have

$$\alpha = h\sigma \oplus \overline{\alpha}$$

where the degree of h is less than or equal to $n - s - 1$, the degree of $\overline{\alpha}$ is less than s. Thus we have defined a mapping from V_n to V_s: $\alpha \rightarrow \overline{\alpha}$.

Now let ξ be a vector in V_n and $\overline{\xi}$ a vector in V_s. Let $F(\overline{\xi})$ be a differentially 2-uniform permutation on V_s. Set $G(\xi) = F(\overline{\xi})$. This gives an $n \times s$ S-box. Note that $\overline{\xi \oplus \eta} = \overline{\xi} \oplus \overline{\eta}$. This means that the mapping from V_n to V_s, $\alpha \rightarrow \overline{\alpha}$, is linear. Hence $G(\xi)$ is not an S-box with a UHODDT, although it is regular (see Subsection 5.1).

Now let $\Phi(\xi)$ be a differentially 2-uniform permutation on V_n. Set $\Psi(\xi) = \overline{\Phi(\xi)}$. Ψ is an $n \times s$ S-box. A similar argument shows that the difference distribution table of $\Psi(\xi)$ is not uniformly half-occupied.

5 Hadamard Matrices Embodied in Difference Distribution Table

In this section we reveal a very important combinatorial property of differentially 2-uniform quadratic permutations, namely, every differentially 2-uniform quadratic permutation is associated with a Sylvester-Hadamard matrix. As an application of the result, we show that chopping a differentially 2-uniform quadratic permutation results in an S-box whose difference distribution table is nearly flat. Such an S-box is very weak to the differential attack.

5.1 Difference Distribution Tables and Incidence Functions

Let $F = (f_1, \ldots, f_n)$ be a differentially 2-uniform quadratic permutation on V_n, namely, a quadratic permutation with a UHODDT or uniformly half-occupied difference distribution table. Let W_α be the set of vectors $F(x) \oplus F(x \oplus \alpha)$ runs through when x runs through V_n, namely,

$$W_\alpha = \{F(x) \oplus F(x \oplus \alpha) | x \in V_n\} \tag{5}$$

Obviously if $\alpha = 0$ then $W_\alpha = \{0\}$. Since each f_j is quadratic $f_j(x) \oplus f_j(x \oplus \alpha)$ is an affine function.

Write $f_j \oplus f_j(x \oplus \alpha) = c_{1j}x_1 \oplus \cdots \oplus c_{nj}x_n \oplus d_j$, $j = 1, \ldots, n$. Set $C_\alpha = (c_{ij})$, $\sigma_\alpha = (d_1, \ldots, d_n)$. Thus $F(x) \oplus F(x \oplus \alpha) = xC_\alpha \oplus \sigma_\alpha$ and $W_\alpha = \{F(x) \oplus F(x \oplus \alpha) | x \in V_n\} = \{xC_\alpha \oplus \sigma_\alpha | x \in V_n\}$.

Now let $\alpha \neq 0$. Since F is a permutation, $F(x) \oplus F(x \oplus \alpha) \neq 0$ for any $x \in V_n$. Hence $0 \notin W_\alpha$. Since $F(0) \oplus F(\alpha) = \sigma_\alpha$, we have $\sigma_\alpha \neq 0$. And by the definition of a UHODDT, $|W_\alpha| = 2^{n-1}$ and hence $rank(C_\alpha) = n - 1$. Thus we have

Lemma 11. *Let F be a differentially 2-uniform quadratic permutation on V_n. If $\alpha \neq 0$ then*

(i) $0 \notin W_\alpha$, (ii) $\sigma_\alpha \neq 0$, (iii) $|W_\alpha| = 2^{n-1}$, and (iv) $rank(C_\alpha) = n - 1$.

Now set $W_\alpha^0 = \{xC_\alpha | x \in V_n\}$. Then we have

Lemma 12. *Let F be a differentially 2-uniform quadratic permutation on V_n. If $\alpha \neq 0$ then $V_n = W_\alpha \cup W_\alpha^0$ and $W_\alpha \cap W_\alpha^0 = \phi$.*

Lemma 13. *Let F be a differentially 2-uniform quadratic permutation on V_n. Let $\alpha \neq 0$. Then the following statements hold:*

(i) If $\beta, \beta' \in W_\alpha$ then $\beta \oplus \beta' \in W_\alpha^0$,
(ii) if $\beta \in W_\alpha$, $\beta' \in W_\alpha^0$ then $\beta \oplus \beta' \in W_\alpha$,
(iii) if $\beta, \beta' \in W_\alpha^0$ then $\beta \oplus \beta' \in W_\alpha^0$.

Let F be a differentially 2-uniform quadratic permutation on V_n and let W_α be the same as (5). For each $\alpha \in V_n$ we define an *incidence function* φ_α as follows:

$$\varphi_\alpha(\beta) = \begin{cases} 0 \text{ if } \alpha = 0 \\ 1 \text{ if } \alpha \neq 0 \text{ and } \beta \in W_\alpha \\ 0 \text{ if } \alpha \neq 0 \text{ and } \beta \notin W_\alpha \end{cases} \tag{6}$$

As is to be proved below, each φ_α is in fact a linear function on V_n.

Lemma 14. *Let F be a differentially 2-uniform quadratic permutation on V_n. Then φ_α, defined in (6), is a linear function on V_n for every vector $\alpha \in V_n$.*

Lemma 15. *Let F be a differentially 2-uniform quadratic permutation on V_n. If $\alpha \neq \alpha'$, then $\varphi_\alpha \neq \varphi_{\alpha'}$.*

5.2 Hadamard Matrices in Difference Distribution Tables

Lemma 14 states that each row of the differential distribution table is associated with a linear function on V_n, while Lemma 15 indicates that these linear functions are all different. Hence we have

Theorem 16. *Let F be a differentially 2-uniform quadratic permutation on V_n. Then φ_α runs through all linear functions on V_n while α runs through the vectors in V_n.*

Recall that $\alpha_0, \alpha_1, \ldots, \alpha_{2^n-1}$ are all the vectors in V_n, with $\alpha_0 = (0, \ldots, 0)$, $\ldots$, $\alpha_{2^n-1} = (1, \ldots, 1)$. Let $M = (m_{ij})$ be a $(1, -1)$-matrix defined by

$$m_{ij} = (-1)^{\varphi_{\alpha_i}(\alpha_j)} \tag{7}$$

M is called the *difference trait matrix* of F. Essentially, M is a matrix obtained from the difference distribution table of the S-box by replacing each zero entry by 1 and each nonzero entry by -1, with an exception that the first entry in the first row is replaced by 1.

Theorem 17. *Let F be a differentially 2-uniform quadratic permutation on V_n. Then M, the difference trait matrix of F, is a Sylvester-Hadamard matrix if the row-order is ignored.*

Proof. From Theorem 16, the 2^n rows of M comprise all the linear sequences of length 2^n. By Lemma 1 of [16], each linear sequence of length 2^n is a row of H_n. Thus M can be changed to H_n by re-ordering its rows.

Obviously, W_α, φ_α and M can be defined for any permutation on V_n, not restricted to quadratic ones.

Theorem 18. *Let F be a differentially 2-uniform quadratic permutation on V_n and M be the difference trait matrix of F. Then the inverse of F is also a differentially 2-uniform permutation, whose difference trait matrix is the transpose of M.*

Note that for a differentially 2-uniform quadratic permutation F based on a cubic polynomial on $GF(2^n)$, n odd, the algebraic degree of F^{-1} is larger than $(n+1)/2$. By Theorem 18, both the difference trait matrix of F and that of F^{-1} are Sylvester-Hadamard matrices (subject to re-ordering their rows).

5.3 Chopping Quadratic Permutations

Let $F = (f_1, \ldots, f_n)$ be a differentially 2-uniform permutation on V_n. Let G be an S-box obtained by chopping a component function of F, say $G = (f_2, \ldots, f_n)$. Similarly to W_α, φ and M corresponding to F (see (5), (6) and (7)), we can define

$$U_\alpha = \{G(x) \oplus G(x \oplus \alpha) | x \in V_n\},$$

where $\alpha \in V_n$, and the incidence function

$$\psi_\alpha(\beta) = \begin{cases} 0 \text{ if } \alpha = 0 \\ 1 \text{ if } \alpha \neq 0 \text{ and } \beta \in U_\alpha \\ 0 \text{ if } \alpha \neq 0 \text{ and } \beta \notin U_\alpha \end{cases}$$

where $\beta \in V_{n-1}$.

Let $\alpha_0, \alpha_1, \cdots, \alpha_{2^n-1}$ be the ordered vectors in V_n and $\beta_0, \beta_1, \cdots, \beta_{2^{n-1}-1}$ the ordered vectors in V_{n-1}. Define a $2^n \times 2^{n-1}$ (1, -1)-matrix, say $N = (n_{ij})$, where $n_{ij} = (-1)^{\psi_{\beta_i}(\beta_j)}$.

Write $M = [M_1 M_2]$ where each M_j is of order $2^n \times 2^{n-1}$, $M_1 = (m_{ij})$, and $M_2 = (m_{ij+2^{n-1}})$. It is easy to see that $\psi_\alpha(\beta) = 1$ if and only if $\varphi_\alpha(0, \beta) = 1$ or $\varphi_\alpha(1, \beta) = 1$. In other words, $n_{ij} = -1$ if and only if $m_{ij} = -1$ or $m_{ij+2^{n-1}} = -1$.

Since F is a differentially 2-uniform quadratic permutation, by Theorem 17, each row of M is a row of H_n. Now recall that $H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix}$. Write $H_n = (h_{ij})$, $i, j = 1, \ldots, 2^n$. We can see that $-h_{ij} = h_{ij+2^{n-1}}$ if $i > 2^{n-1}$. This implies that $h_{ij} = -1$ or $m_{ij+2^{n-1}} = -1$, if $i > 2^{n-1}$. Note that M and H_n have the same set of rows. This proves that there exists 2^{n-1} nonzero $\alpha \in V_n$ such that ψ_α is constant 1. In this case $G(x) \oplus G(x \oplus \alpha)$ runs through every vector (including the zero vector) in V_{n-1}, for some 2^{n-1} nonzero vectors $\alpha \in V_n$ and hence the robustness of G is less than $\frac{1}{2}$.

To summarize the above discussions, the difference distribution table of an S-box obtained by chopping a component function of a differentially 2-uniform quadratic permutation has the following profile: it can be viewed as a folded (right to left) version of the uniformly half-occupied table of the original permutation, with half of the rows containing a value 2 in all their entries, and the remaining rows, not counting the first row, containing an equal number of 0s and 4s. Similarly, chopping two component functions from a permutation results in an S-box whose difference distribution table is almost flat: it can be viewed as a twice-folded (right to left) version of the uniformly half-occupied table of the original permutation, and three quarters of the rows contain a value 4 in all their entries, while the remaining rows, not counting the first row, have an equal number of 0s and 8s. This observation can be extended to the case when three or more component functions are chopped.

In conclusion, S-boxes obtained by chopping differentially 2-uniform quadratic permutations have an almost flat difference distribution table, which renders a DES-like encryption algorithm that employs such S-boxes very prone to the differential attack.

Acknowledgments The first author was supported in part by the Australian Research Council under the reference numbers A49130102, A49131885 and A49232172, the second author by A49130102, and the third author by A49232172. All authors were supported by a University of Wollongong Research Program grant and the first two by ATERB C010/058. The authors would like to thank the anonymous referees for Crypto'94 for their helpful comments.

References

1. Adams, C. M.: On immunity against Biham and Shamir's "differential cryptanalysis". Information Processing Letters 41 (1992) 77–80

2. Beth, T., Ding, C.: On permutations against differential cryptanalysis. In Advances in Cryptology - EUROCRYPT'93 (1994) vol. 765, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 65–76
3. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology **Vol. 4, No. 1** (1991) 3–72
4. Biham, E., Shamir, A.: Differential Cryptanalysis of the Data Encryption Standard. Springer-Verlag New York, Heidelberg, Tokyo 1993
5. Brown, L., Kwan, M., Pieprzyk, J., Seberry, J.: Improving resistance to differential cryptanalysis and the redesign of LOKI. In Advances in Cryptology - ASIACRYPT'91 (1993) vol. 739, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 36–50
6. Dillon, J. F.: A survey of bent functions. The NSA Technical Journal (1972) 191–215
7. Matsui, M.: Linear cryptanalysis method for DES cipher. In Advances in Cryptology - EUROCRYPT'93 (1994) vol. 765, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 386–397
8. Matsui, M.: Linear cryptanalysis method for DES cipher (II). In Proceedings of 1994 Symposium on Cryptography and Information Security (Japan, 1994)
9. Nyberg, K.: Perfect nonlinear S-boxes. In Advances in Cryptology - EUROCRYPT'91 (1991) vol. 547, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 378–386
10. Nyberg, K.: On the construction of highly nonlinear permutations. In Advances in Cryptology - EUROCRYPT'92 (1993) vol. 658, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 92–98
11. Nyberg, K.: Differentially uniform mappings for cryptography. In Advances in Cryptology - EUROCRYPT'93 (1994) vol. 765, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 55–65
12. Nyberg, K., Knudsen, L. R.: Provable security against differential cryptanalysis. In Advances in Cryptology - CRYPTO'92 (1993) vol. 740, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 566–574
13. Pieprzyk, J.: Bent permutations. In Proceeding of the International Conference on Finite Fields, Coding Theory, and Advances in Communications and Computing (Las Vegas, 1991)
14. Rothaus, O. S.: On "bent" functions. Journal of Combinatorial Theory **Ser. A, 20** (1976) 300–305
15. Seberry, J., Zhang, X. M., Zheng, Y.: Systematic generation of cryptographically robust S-boxes. In Proceedings of the first ACM Conference on Computer and Communications Security (1993) The Association for Computing Machinery, New York pp. 172 – 182
16. Seberry, J., Zhang, X. M., Zheng, Y.: Nonlinearly balanced boolean functions and their propagation characteristics. In Advances in Cryptology - CRYPTO'93 (1994) vol. 773, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 49–60
17. Seberry, J., Zhang, X. M., Zheng, Y.: Relationships among nonlinearity criteria. Presented at *EUROCRYPT'94*, 1994

L Number	Hits	Search Text	DB	Time stamp
-	1	lahtinen.in. and seed adj number	DERWENT	2004/04/19 07:43
-	161	s adj box	US-PGPUB	2004/04/19 10:04
-	804	s adj box	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/19 10:05
-	77	(s adj box) and key$3 with s$1box	USPAT; US-PGPUB; EPO; JPO; DERWENT	2004/04/19 11:44
-	2	(s adj box) and keyed with s$1box	USPAT; US-PGPUB; EPO; JPO; DERWENT	2004/04/19 10:11
-	11	(s adj box) and keyed and s$1box	USPAT; US-PGPUB; EPO; JPO; DERWENT	2004/04/19 11:04
-	15	(s adj box) and auto$3 and s$1box	USPAT; US-PGPUB; EPO; JPO; DERWENT	2004/04/19 11:29
-	1	plain$4 adj text with key$3 with s$1box	USPAT; US-PGPUB; EPO; JPO; DERWENT	2004/04/19 11:34
-	3	plain$4 adj text with key$3 with s adj box	USPAT; US-PGPUB; EPO; JPO; DERWENT	2004/04/19 11:35
-	102	s$1box	US-PGPUB	2004/04/19 11:39
-	97	(s adj box) and key$3 with (s adj box or s$1box)	USPAT; US-PGPUB; EPO; JPO; DERWENT	2004/04/19 11:41
-	1		USPAT; US-PGPUB; EPO; JPO; DERWENT	2004/04/19 11:42
-	31	((s adj box) and key$3 with s$1box) and @ay<2000	USPAT; US-PGPUB; EPO; JPO; DERWENT	2004/04/19 11:45